

S50V Quick Reference

Version 2.5.1.0

February 2007

101-00242-00



FORCE  TM

Copyright 2007 Force10 Networks

All rights reserved. Printed in the USA, February 2007.

Force10 Networks reserves the right to change, modify, revise this publication without notice.

Trademarks

Copyright 2007 by Force10 Networks, Inc. All rights reserved. Force10 Networks® and E-Series® are registered trademarks of Force10 Networks, Inc. Force10, the Force10 logo, E1200, E600, E300, EtherScale, FTOS, S-Series, SFTOS, and TeraScale are trademarks of Force10 Networks, Inc. All other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Force10 Networks reserves the right to make changes to products described in this document without notice.

USA Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designated to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance to the instructions, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures necessary to correct the interference at their own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Force10 Networks is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications in the equipment. Unauthorized changes or modification could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communication Statement

The digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Attention: Le présent appareil numérique n'émet pas de perturbations radioélectriques dépassant les normes applicables aux appareils numériques de la Class A prescrites dans le Règlement sur les interférences radioélectriques établi par le ministère des Communications du Canada.

European Union EMC Directive Conformance Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. Force 10 Networks can not accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of this product, including the fitting of non-Force10 option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/ European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.



Warning: This device is a Class A product. In a domestic environment, this device can cause radio interference, in which case, the user may be required to take appropriate measures.

VCCI Compliance for Class A Equipment (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is Class A product based on the standard of the Voluntary Control Council For Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.



Danger: AC Power cords are for use with Force10 Networks equipment only, do not use Force10 Networks AC Power cords with any unauthorized hardware.

本製品に同梱いたしております電源コードセットは、本製品専用です。
本電源コードセットは、本製品以外の製品ならびに他の用途でご使用いただくことは出来ません。製品本体には同梱された電源コードセットを使用し、他製品の電源コードセットを使用しないで下さい。

Feedback on Documentation?
Send email to techpubs@force10networks.com

Contents

Overview	4
Contents of the S-Series Documentation CD-ROM	5
Installing the Hardware	6
Component Overview	6
Inserting 10-Gigabit and Stacking Modules (optional)	6
Attaching the S50V to the Rack	7
Connecting Stacking Ports (optional)	8
Installing SFP Modules (optional)	9
Installing XFP Modules (optional)	10
Connecting a Cable to the Console Port	10
Connecting Ethernet Ports with PoE	11
Basic Software Configuration	11
Creating a User and Password	12
Setting the Enable Password	12
Enabling Ports	12
Setting the Management IP Address	13
Enabling Telnet to the Switch	13
Managing a Stack of S-Series Switches	14
Installing New Software	14
Enabling and Using the SFTOS Web User Interface	15
Creating a Simple Configuration using VLANs and STP	16
Enabling Spanning Tree Protocol	17
Notable Differences between S-Series and E-Series	19
Interface Nomenclature	19
The iSupport Website	20

Overview

Thank you for purchasing a Force10 Networks switch!

This *S50V Quick Reference* document is printed and included in the S50V shipping box to provide you with a quick way to access basic installation and configuration instructions and to tell you how to get more information.

In addition to the S50V with its SFTOS operating system loaded in its default configuration, the shipping box also contains the AC power cord, a DB9 to RJ45 connector, and a small bag with rack-mounting screws, plastic feet for table-top mounting, and the *S-Series Documentation* CD-ROM (hereafter simply referred to as the “S-Series CD-ROM”).

Other purchased components are shipped separately.

The hardware installation section ([Installing the Hardware on page 6](#)) in this guide contains a subset of the information in *Installing the S50V System*, a book stored as a PDF both on the S-Series CD-ROM and at the iSupport website.

The software configuration section here (see [Basic Software Configuration on page 12](#)) contains a subset of the configuration information in the *SFTOS Configuration Guide*, which is also on the S-Series CD-ROM and at the iSupport website.

In fact, all of the S-Series documentation that is on the S-Series CD-ROM is also available on the iSupport website.

For more information about the S-Series CD-ROM, see the next section, [Contents of the S-Series Documentation CD-ROM on page 5](#).

For more information about the iSupport website (login required), see [The iSupport Website on page 21](#).



Note: This *S50V Quick Reference* is specific to SFTOS Version 2.5.1 for the S50V.

Contents of the S-Series Documentation CD-ROM

The S-Series Documentation CD-ROM launches a Web page from the CD-ROM containing the links described in the following sections:

Force10 Literature: This is a link to the Force10 Literature folder on the CD-ROM. It contains links to data sheets for all Force10 products.

Installing the S50 System: This book contains details of installation options for the S50 model.

Installing the S50V System: This book contains details of installation options for the S50V model.

S50V Quick Reference for SFTOS 2.5.1: This book is a PDF version of this book, which is included in the S50V shipping box.

S50 Quick Reference for SFTOS 2.5.1: This book is a PDF version of the book that is included in the S50 shipping box.

SFTOS Command Reference: This book contains syntax statements for all SFTOS commands in both the Layer 2 and Layer 3 packages.

SFTOS Configuration Guide: This book is designed to help you perform the most common configuration tasks, with examples of the most commonly used commands.

MIBs: This is a link to a folder on the CD-ROM containing the S-Series MIBs, updated for 2.5.1.

Secure Communications (SSH/SSL/HTTPS): This link opens an HTML page containing a link to the *S-Series Secure Management* application note on the CD, describing how to enable secure communications through SSH, SSL, and HTTP. The page also contains links to folders on the CD-ROM containing example keys and shell scripts that you can use to generate your own SSH keys and SSL certificates.

The **Training Material** link on the CD-ROM home page is to a folder on the CD-ROM containing sets of slides, in PDF format, that are used in the S-Series training, updated for 2.5.1.



Note: The SFTOS software and the S-Series Release Notes, which had been on previous versions of the S-Series CD-ROM, are no longer on the CD-ROM. The iSupport website of Force10 contains the most recent software and documents. For details, see [The iSupport Website on page 21](#).

Installing the Hardware



Danger: To prevent electrical shock, make sure the S50V is grounded properly. If you do not ground your equipment correctly, excessive emissions may result. Use a qualified electrician to ensure the power cables meet your local electrical requirements.

To install the S50V system, Force10 Networks recommends that you complete the installation procedures in the order presented below, before attaching a power source:

- Insert 10-Gigabit and Stacking Modules (optional). See [Inserting 10-Gigabit and Stacking Modules \(optional\) on page 6](#).
- Attach the S50V to the Rack. See [Attaching the S50V to the Rack on page 8](#).
- Connect Stacking Ports (optional). See [Connecting Stacking Ports \(optional\) on page 8](#).
- Connect to the Console Port. See [Connecting a Cable to the Console Port on page 11](#).
- Connect Ethernet Ports. See [Connecting Ethernet Ports with PoE on page 11](#).



Warning: As with all electrical devices of this type, take all the necessary safety precautions to prevent injury when installing this system. Electrostatic discharge (ESD) damage can occur if components are mishandled. Always wear an ESD-preventive wrist or heel ground strap when handling the switch and its components.

Warning: Before starting the installation, be sure that the installation conditions conform to those specified in *Installing the S50V System*.

Component Overview

The following sections in this *S50V Quick Reference* contain basic information on several optional modules. For more on the components of the S50V, see *Installing the S50V System*, on the S-Series CD-ROM.

To manage the switch, you first access the S50V through its console port (see [Connecting a Cable to the Console Port on page 11](#)), where you use the SFTOS Command Line Interface (CLI) to enable ports (see [Connecting Ethernet Ports with PoE on page 11](#).) All ports are in the management VLAN by default, so you can access the CLI through any active ports (see [Basic Software Configuration on page 12](#).)

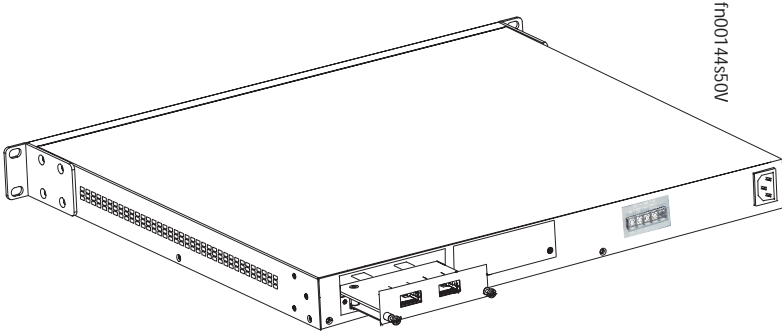
Inserting 10-Gigabit and Stacking Modules (optional)

The S50V has two expansion slots in the back of the chassis, for which there are four types of module available:

- Two types of stacking module: 12 Gbps and 24 Gbps
- Two types of 10-Gigabit module: fiber (optical) and copper (10GBase-CX4)

The system supports inserting the modules in any combination of slots, although connecting all four ports of two 12G stacking modules is not supported, nor is connecting one kind of stack port to anything other than the same kind of stack port. For the 10-Gigabit modules, the system numbers the ports 49 and 50 in the left-hand slot and 51 through 52 in the right-hand slot as you face the front of the switch. So, for clarity in the use of the CLI in port assignment, if you are only using one XFP or CX4 module, insert it in the left-most expansion slot.

To install a module, follow the steps below:

Step	Task
1.	<p>If the switch is on, save the running config, if desired (and different from the startup configuration), with the command write memory. Then power down the S50V by unplugging it from its power source.</p> <p>Caution: Removing a module from a running S50V will crash and lock up the switch, requiring a power cycle.</p>
2.	<p>Use a #2 Phillips screwdriver to remove either a module faceplate or an existing module. Note that these slots, when used for 10G Ethernet ports, are assigned port numbers from left to right as you face the front of the switch. So, for clarity in programming ports, you might favor using the left-most slot for the first 10G module.</p>
3.	<p>Grasping the module faceplate, remove the module from its packaging and slide it into the slot until the module faceplate is flush with the switch.</p> 
4.	<p>Secure the captive screws on either side of the module.</p>
5.	<p>The optical XFP 10-Gigabit module (Catalog # S50-01-10GE-2P) requires additional XFP transceiver inserts, which are not included in the module kit (see Installing XFP Transceivers (optional) on page 10 or the installation instructions that come with the transceiver). The ports in the copper CX4 module (Cat # S50-01-10GE-2C) do not require inserts.</p> <p>If you are installing a CX4 module, and you are connecting the ports with a cable substantially shorter or longer than 5m, use the cx4-cable-length command to set the signal strength. Use cx4-cable-length long for a longer cable, cx4-cable-length short for a shorter cable. See the System Management Commands chapter in the <i>SFTOS Command Reference</i> for details.</p> <p>Note: Take care not to connect CX4 ports to 12G stack ports in the S50V and S25P. The receptacles and cables are the same, but they are incompatible. CX4 ports are labeled as such; stack ports are not labeled. You can order several cable lengths of each type; they are not part of this kit.</p> <p>For details on enabling ports, see Enabling Ports on page 13 or the <i>SFTOS Configuration Guide</i>.</p>

Attaching the S50V to the Rack



Warning: As with all electrical devices of this type, take all necessary safety precautions to prevent injury when installing the system. Electrostatic discharge (ESD) damage can occur if components are mishandled. Always wear an ESD-preventive wrist or heel ground strap when handling the switch and its components.

Warning: For fan maintenance and proper ventilation, position the switch in an equipment rack (or cabinet) with a minimum of five inches (12.7 cm) of clearance around the side intake and exhaust vents.

Warning: The site where the switch is placed should be a dry, clean, well-ventilated, and temperature-controlled room, away from heat sources such as hot air vents or direct sunlight, and have an environmental temperature between 32° – 122°F (0° – 40°C).

The S50V is shipped with universal front-mounting brackets (rack ears) attached. The screws for attaching those ears to a standard 19-inch rack are in the bag that also contains the S-Series CD-ROM.

Position the S50V chassis in the rack. Secure the chassis with two screws through each bracket and onto the rack post.

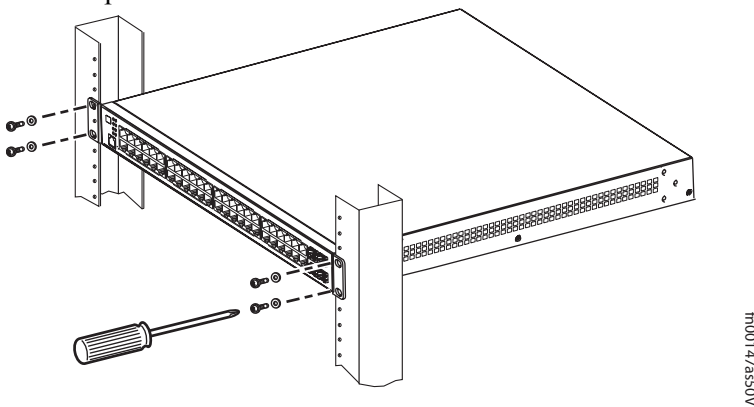


Figure 1 Front-mounting the S50V



Note: The front-mounting installation above is one of several installation options contained in the book *Installing the S50V System*. Other options include rear mounting, four-post mounting, and table-mounting.

Connecting Stacking Ports (optional)

You can connect up to eight switches (S25P and S50V) together through their stack ports to configure them to act as a unified system, called a stack.



Note: The original S50 model stacks only with other switches of that model.

The S50V contains two expansion slots in the rear, in either of which you can insert stacking modules. The S50V system includes two optional types of stacking module — a single-port 24G module and a two-port 12G module. You can put either type of module in either of the two slots in the rear of the S25P, but you cannot interconnect the two types, and Force10 does not support the use of all four ports of two 24G modules.

Use the optional stacking cables to connect the switches through the stacking ports. One possible configuration is depicted below.



Note: Figure 2 on page 9 shows a connection between the top and bottom switches, from Stack Port A on unit 1 to Stack Port B on unit 3. That connection completes a topology called a ring. That ring is not necessary, because the ports are bi-directional, but a ring provides redundancy in case of a failure of a stacking cable or port. If you use the single-port 24G modules, you can insert one in each expansion slot to accomplish the ring topology.

Note: These instructions use “Stack Port A” and “Stack Port B” for clarifying the connections, but the modules are not labeled.

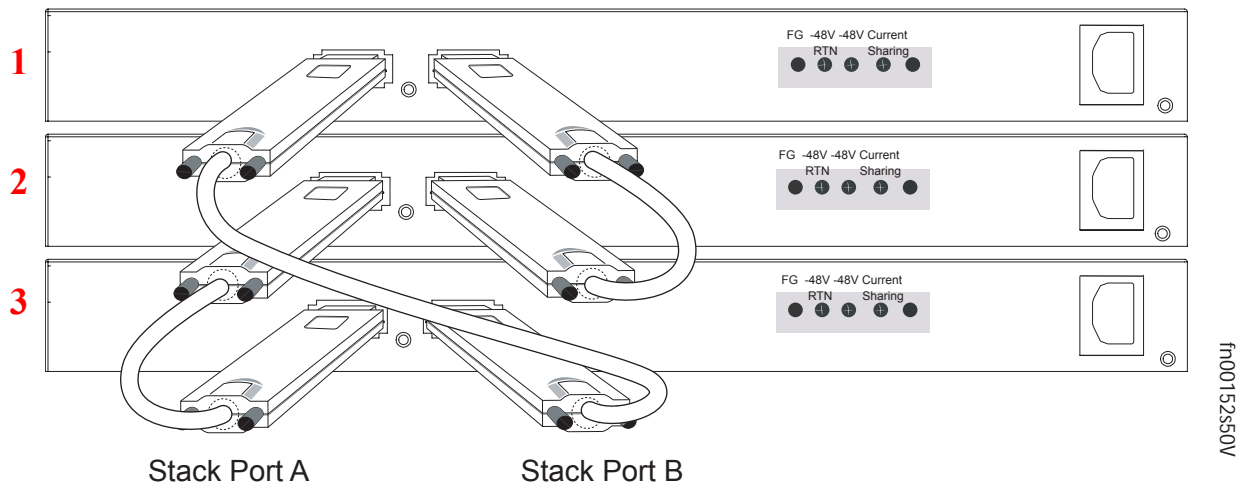
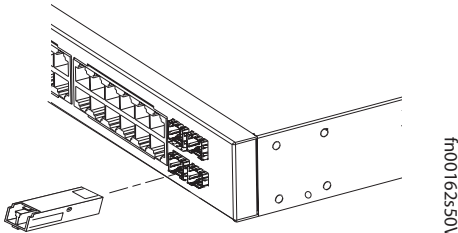


Figure 2 Connecting Stack Ports



Note: The connectors in Figure 2 are depicted with captive screws. Instead, the connectors used on S50V stack ports have latches, the same connectors as used for CX4 connections.

Installing SFP Transceivers (optional)

<p>To install 1Gbps SFPs (Small Form-factor Pluggable optical transceivers) into the four open ports at the right front of the S50V:</p> <ol style="list-style-type: none"> 1. Position the SFP so that the bail is closed and on top of the SFP. 2. Insert the SFP into the port until it gently snaps into place. 	 <p>fn00162s50v</p>	<p>Note: The four SFP ports shown in the graphic, when populated, automatically preempt the four copper ports labeled 45 through 48. In other words, while you use a particular optical port, you cannot use the equivalent copper port.</p>
---	---	--

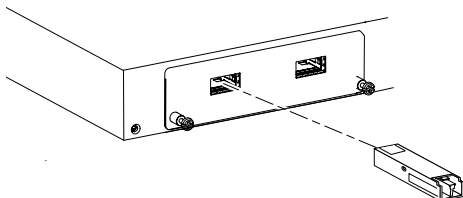


Note: For details on SFP and XFP optics supported by Force10, see <http://www.force10networks.com/products/specifications.asp>

Installing XFP Transceivers (optional)



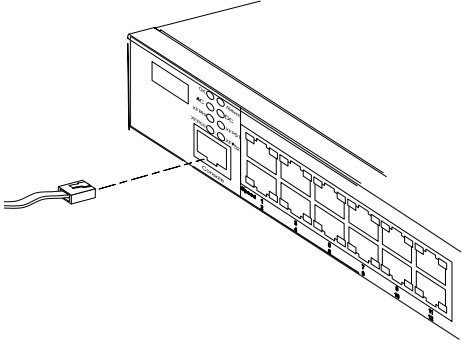
Warning: Do not look directly into any optical port. Failure to follow this warning could result in physical harm.

<p>The two module slots on the back of the S50V both accept optional 10-Gigabit modules.</p> <p>To install an XFP transceiver into an XFP port (in the fiber optical version of the 10-Gigabit module):</p> <ol style="list-style-type: none"> 1. Position the XFP so that the bail is closed and on top of the XFP. 2. Insert the XFP into the port until it gently snaps into place. 	
--	--

Connecting a Cable to the Console Port



Caution: Install a **straight-through RJ-45 copper cable** (a standard Ethernet cable) into the console port. This is different from many other implementations that require a crossover cable (or rollover cable). If connecting to a terminal server and using an Ethernet crossover cable, daisychain another crossover cable to effectively get a straight-through cable connection. Many console terminal servers use octopus cables that are crossover cables. As above, connect an additional crossover cable.

<p>Connect the RJ-45/DB-9 adapter that is shipped with the S50V system to the RJ-45 cable.</p> <p>Console port pinout:</p> <ul style="list-style-type: none">Pin 1 = NCPin 2 = NCPin 3 = RXDPin 4 = GNDPin 5 = GNDPin 6 = TXDPin 7 = NCPin 8 = NC		<p>Set your initial console terminal settings to:</p> <ul style="list-style-type: none">• 9600 baud rate• no parity• 8 data bits• 1 stop bit• no flow control <p>After establishing a connection, you can modify the settings to match at each end of the connection.</p>
--	---	---

See the Getting Started chapter of the *SFTOS Configuration Guide* for other console port details, such as setting the console timeout and the baud rate.

Connecting Ethernet Ports with PoE

The copper ports (ports 1 through 48) in the S50V are enabled by default to deliver power to connected powered devices that follow the IEEE 802.3af specification for Power over Ethernet (PoE). For delivering PoE, use the same Cat. 5 cables and RJ-45 connectors that you use for non-PoE connections.

Although the power controller can deliver up to 360 watts, the 470 watt power supply will limit PoE power to 320 watts if the switch requires power for other uses. The default PoE configuration limits PoE power to 288 watts.

So, while each port can provide more than the maximum of 15.4 watts required by the IEEE 802.3af specification, the available power to a particular port is subject to the power budget of the switch and to the power already allotted to other ports. If you expect that the powered devices connected to one switch will require more than a total of 320 watts, you can use the command line interface (CLI) to prioritize the allocation of power and to raise the power budget threshold.

To determine the status of PoE power on the switch and to individual ports, use:

show inlinepower {*unit/slot/port* | **all**} (Privileged Exec mode)

Some commands that you can use to manage the PoE power budget include:

- **inlinepower limit** 1-20 (Interface Config mode): Set a power limit on the port.
- **inlinepower priority** {critical | high | low} (Interface Config mode): Set a PoE priority on the port.
- **inlinepower threshold** 0-100 unit-id (Global Config): Override the 80% default limit of the PoE power budget.

For more on CLI commands that control PoE, see the PoE sections of the System Configuration chapter in the *SFTOS CLI Reference* and the Configuring Interfaces chapter in the *SFTOS Configuration Guide*. Also, in this guide, see [Enabling Ports on page 13](#).

Basic Software Configuration

This *S50V Quick Reference* contains a small subset of the information that is provided in the Getting Started chapter of the *SFTOS Configuration Guide*. That guide is available PDF format on the S-Series CD-ROM and on the Documents tab of the iSupport website.

This section discusses the following configuration topics for the S50V:

- [Creating a User and Password on page 13](#)
- [Setting the Enable Password on page 13](#)
- [Enabling Ports on page 13](#)
- [Setting the Management IP Address on page 14](#)
- [Enabling Telnet to the Switch on page 14](#)
- [Managing a Stack of S-Series Switches on page 15](#)
- [Installing New Software on page 15](#)
- [Enabling and Using the SFTOS Web User Interface on page 16](#)

Creating a User and Password

The S50V comes installed with one read/write user named “admin”, with no password. You can add that password, and also create up to five more read/write users with the **username** command in Global Config mode. The command edits the user name and password in one statement, as shown below. Usernames provide access to the S50V through both the CLI and the SFTOS Web User Interface (Web UI).



Note: Text boxes surrounded by oval lines, such as the following, are used throughout Force10 documentation to simulate the appearance of a terminal screen after logging in to the operating system of the switch through a console program. The hostname prompt, exemplified in the following example by “(Force10)”, is configurable.

Note: In this guide, bold text highlights the commands that you enter.

```
(Force10) >enable
(Force10) #config
(Force10) (Config) #username admin passwd apassword
User login name and password are set.
(Force10) (Config) #exit
(Force10) #exit
(Force10) >
```

Setting the Enable Password

The Privileged Exec password (commonly called the “enable” password), is not set when the switch starts the first time. To set the enable password, access the Privileged Exec mode (also called “enable mode”) and then the Global Config mode, as shown in the following example. Enter the command **enable passwd**, then press **Enter**.

At the prompts, enter the password that you want to use:

```
(Force10) >enable
(Force10) #enable passwd
Enter new password:*****
Confirm new password:*****
Password Changed!
(Force10) #exit
```

Enabling Ports

When the switch is first installed, all ports are disabled by default. To enable all ports, enter **no shutdown all** in Global Config mode, as shown here:

```
(Force10) >enable
(Force10) #config
(Force10) (Config) #no shutdown all
(Force10) (Config) #exit
```

Alternatively, you can use the **no shutdown** command at the specific interface level.



Note: The equivalent action on the Web UI is to select **Enable** in the Admin Mode field of the Port Configuration panel. See [Enabling and Using the SFTOS Web User Interface on page 16](#).

Note: The S50V supports IEEE 802.3af, the Power over Ethernet (PoE) standard for sending power through the copper ports. For more on PoE, see [Connecting Ethernet Ports with PoE on page 11](#).

Setting the Management IP Address

Use the following the procedure to set up a management IP interface to the switch. You will need this to access the switch through Telnet, SSH, TFTP, or the SFTOS Web User Interface.

Step	Command Syntax	Command Mode	Purpose
1.	show interface managementethernet	User Exec or Privileged Exec	Display current management IP configuration.
2.	interface managementethernet	Global Config	Invoke the (Config-if-ma)# prompt.
3.	ip address ipaddr subnetmask	(Config-if-ma)# prompt within the Global Config mode	Set the IP address and subnet mask of the management interface.
4.	management route default gateway	Global Config	Set the IP gateway of the management interface.



Note: The management address is reachable from VLAN 1. All physical ports are, by default, members of VLAN 1, so the management address will be reachable from all enabled physical ports by default.

Enabling Telnet to the Switch

Access to the switch through a Telnet server is disabled by default. If you want to access the switch through an SSH client, you would leave Telnet disabled and set up the SSH connection, as described in “Enabling Secure Management with Secure Shell or Secure Sockets Layer” in the *SFTOS Configuration Guide*.

To enable Telnet access, first assign the management IP address (see [Setting the Management IP Address on page 14](#)), then execute the **ip telnet server enable** command in Global Config mode.

Managing a Stack of S-Series Switches

When you connect a set of previously unconfigured S-Series switches, and you follow the instructions in [Connecting Stacking Ports \(optional\) on page 8](#), a startup algorithm automatically designates a unit to be the management unit. You do not need to configure anything else specific to stack management.

If, on the other hand, you are modifying a stack, you will need to follow the directions that are in the Stacking chapter of the *SFTOS Configuration Guide*.

If you need to upgrade the software in the stack, see the following section.

Installing New Software

As a convenience to purchasers of the SFTOS Layer 3 Package, the S50V comes with that software already installed. So, other than checking the iSupport website for upgrades, you do not need to download new code. The Layer 3 software package includes the Layer 2 package, so if you purchased just the Layer 2 package, your software license proscribes using the Layer 3 functionality. That is easy to do; simply do not execute the **routing** command (Global Config mode); the Layer 3 functionality will be unavailable.

If you need to upgrade the SFTOS software, and you want to download the software from a TFTP server, use the following command syntax:

```
copy tftp://tftp_server_ip_address/path/filename {image1 | image2}
```

For example: `copy tftp://1.1.1.10/tftp/SFTOSdownload/SFTOS-S50-2.5.1.11.bin image2`

In this example:

- 1.1.1.10 is the IP address of your TFTP server.
- tftp/SFTOSdownload/ is the path to the software.
- SFTOS-S50-2.5.1.6.bin is the software label.
- image2 is the name of the storage location on your switch.

The choice of **image1** or **image2** is based on the fact that SFTOS 2.5.1 introduces support for two software image locations on the switch. The software shipped on the switch is stored in the image1 location, so if you download new software to the image1 location, the next reload will boot up with that software. If you save the new software to the image2 location, as shown above, and you want to install that new software on the next reload, execute the command **boot system image2** before executing **reload**.

You can use variations of the **copy** command to download or upload files to and from the switch. For details on the command syntax, see the **copy** command in the *SFTOS Command Reference*. For more on managing software and configuration files, see “Managing Configuration and Software” in the Getting Started chapter of the *SFTOS Configuration Guide*. Also see “Upgrading Software in a Stack” in the Stacking chapter.

Enabling and Using the SFTOS Web User Interface

The SFTOS Web User Interface (Web UI), provided by SFTOS, provides most of the functionality of the CLI. Also, the CLI and Web UI can be used in combination to give you even better control.

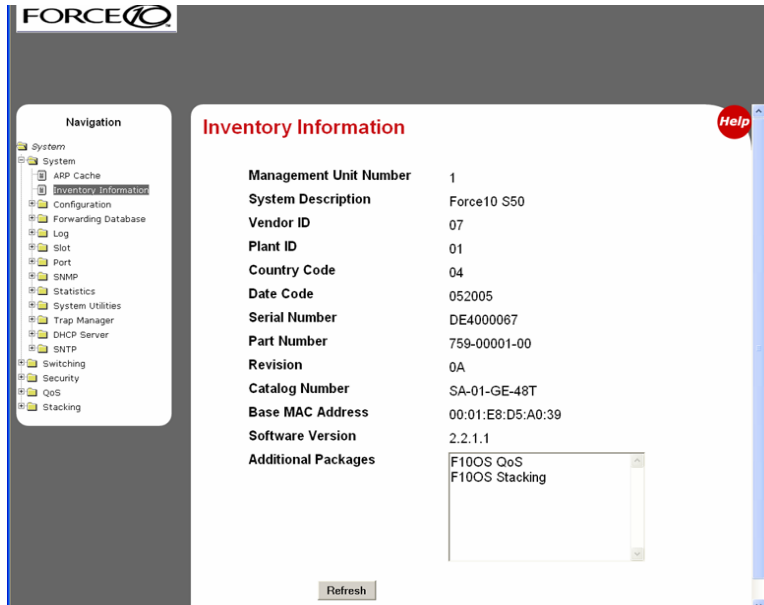
1. To enable the Web UI, you first must give the switch a management IP address. See [Setting the Management IP Address on page 14](#).
2. Then, in Global Config mode, enter the command **ip http server enable**.



Note: Details on enabling an HTTPS secure server are in Chapter 9, “Providing User Access Security”, in the *SFTOS Configuration Guide*, and through the *Secure Communications* link on the S-Series CD-ROM.

3. Launch a supported Web browser. The Web browser must support:
 - HTML version 4.0, or later
 - HTTP version 1.1, or later
 - JavaScript^(TM) version 1.2, or later
4. Enter the URL of the switch (<http://<IP address>>) in the Web browser address field. The IP address is the management IP address that you assigned above.
5. When the Login panel is displayed, click the **Login** button.
6. Enter the admin username and password, or any other username and password that you created, as discussed above in [Creating a User and Password](#).
7. The Navigation tree is displayed in the left frame, and the System Description panel is displayed in the right frame. Make your selection by clicking on the appropriate item in the Navigation tree.

For example, the following screenshot shows that the Inventory Information panel opened when the user clicked the Inventory Information node in the tree. Notice that the Inventory Information panel displays the serial number of the switch. Notice also the large red Help button, which displays on every panel, and provides context help for the panels in the selected branch of the tree.



Creating a Simple Configuration using VLANs and STP

The following is an example of using the command line interface (CLI) to create VLAN 55, adding both a tagged interface and an untagged interface to it (ports 5 and 6, respectively, in stack member unit 1):



Note: As noted in [Enabling Ports on page 13](#), all ports are disabled by default. Enable them with **no shutdown all** (Global Config mode), or individually with the **no shutdown** command on each port (Interface Config mode). The equivalent action on the Web UI is to select **Enable** in the Admin Mode field on the Port Configuration panel.

```
(Force10) (Config) #interface vlan 55
(Force10) (Conf-if-vl-55) #tagged 1/0/5
(Force10) (Conf-if-vl-55) #untagged 1/0/6
(Force10) (Conf-if-vl-55) #exit
(Force10) (Config) #no shutdown all
```

For more on using the CLI to create VLANs, see the VLANs chapters in the *SFTOS Command Reference* and *SFTOS Configuration Guide*.

Enabling Spanning Tree Protocol

Spanning Tree Protocol (STP) is disabled by default. To use the Web UI to enable it, navigate to the **Spanning Tree** branch, and then select the **Switch Configuration/Status** panel:

The screenshot shows the Force10 Web UI. On the left is a navigation tree with categories like Ping, Trap Manager, DHCP Server, SNMP, Switching, VLAN, Protocol-based VLAN, GARP, IGMP Snooping, Port Channel, Multicast Forwarding Data, Spanning Tree, Class of Service, Routing, Security, QoS, and IP Multicast. The 'Spanning Tree' category is expanded, showing sub-items: Switch Configuration/Status, CST Configuration/Status, MST Configuration/Status, CST Port Configuration/Status, MST Port Configuration/Status, and Statistics. The 'Switch Configuration/Status' panel is selected. It has a red 'Help' button in the top right. The panel contains the following fields: 'Spanning Tree Admin Mode' set to 'Enable', 'Force Protocol Version' set to 'IEEE 802.1s', 'Configuration Name' set to '00-01-E8-D5-A0-F7', 'Configuration Revision Level' set to '0' (with a range of 0 to 65535), and 'Configuration Digest Key' set to '0xac36177f50283cd4b83821d8ab26de62'. There are 'Submit' and 'Refresh' buttons. Below these is a table with three columns: MST ID, VID, and FID. The table contains one row: CST, 1, 1.

MST ID	VID	FID
CST	1	1

Select **Enable** next to **Spanning Tree Admin Mode**, above. Then click **Submit**.

Next, enable STP on the desired ports. To use the Web UI, select the **CST Port Configuration/Status** panel. Choose the port from the **Unit/Slot/Port** list, and then set **Port Mode** to **Enable**:

The screenshot shows the Force10 Web UI with the 'CST Port Configuration/Status' panel selected. The panel contains the following fields: 'Unit/Slot/Port' set to '1/0/1', 'Port Priority' set to '128' (range 0 to 240), 'Admin Edge Port' set to 'Disable', 'Port Path Cost' set to '200000' (range 0 to 200000000, 0 = Auto), 'Auto-calculate Port Path Cost' set to 'Enabled', 'Hello Timer' set to '0' (range 1 to 10), 'External Port Path Cost' set to '200000' (range 0 to 200000000, 0 = Auto), 'Auto-calculate External Prt Path Cost' set to 'Enabled', 'Port ID' set to '80:01', 'Port Up Time Since Counters Last Cleared' set to '0 day 0 hr 13 min 16 sec', 'Port Mode' set to 'Enable', and 'Port Forwarding State' set to 'Forwarding'.

Alternatively, you can use the CLI to enable STP. It is possible to enable spanning tree globally, and on all the ports with just two commands:

```
(Force10) #configure
(Force10) (Config)#spanning-tree
(Force10) (Config)#spanning-tree port mode enable all
(Force10) (Config)#exit
(Force10) #show spanning-tree summary

Spanning Tree Adminmode..... Enabled
Spanning Tree Version..... IEEE 802.1s
Configuration Name..... 00-01-E8-D5-A0-F7
Configuration Revision Level..... 0
Configuration Digest Key.....
0xac36177f50283cd4b83821d8ab26de62
Configuration Format Selector..... 0
No MST instances to display.

(Force10) #show spanning-tree interface 1/0/1
Hello Time..... 0
Port Mode..... Enabled
Port Up Time Since Counters Last Cleared..... 0 day 0 hr 19 min 38 sec
STP BPDUs Transmitted..... 2
STP BPDUs Received..... 593
RSTP BPDUs Transmitted..... 0
RSTP BPDUs Received..... 0
MSTP BPDUs Transmitted..... 4
MSTP BPDUs Received..... 0

(Force10) #write memory
![Your final step is to execute the write memory command to save the configuration.]!
```

Notable Differences between S-Series and E-Series

This section describes the major differences in how command usage on the S-Series differs from the E-Series. Users familiar with the E-Series CLI will notice enough similarities in the CLI environment on the S-Series that they can quickly learn the variations in syntax and usage.

Of course, there are more commands with more detailed options in FTOS than in SFTOS, because FTOS runs the E-Series switches, which are more complex than the S-Series line supported by SFTOS.

Interface Nomenclature

The major difference between SFTOS and FTOS is that commands that contain a parameter in the form *slot/port* in FTOS use a *unit/slot/port* parameter in SFTOS for both physical and logical interfaces.

For physical identifiers, the unit is the stack member number in an S-Series stack. For example, both FTOS and SFTOS have the **show interface** command, but the SFTOS equivalent of **show interface gigabitethernet 2/11** (slot 2, port 11 in FTOS) would be **show interface 1/0/11**, where 1/0/11 represents unit 1 in the stack, slot 0, port 11. If the port were in unit 2 of the S-Series stack, the command would be **show interface 2/0/11**.

Logical interface identifiers are automatically generated by SFTOS. They also use the unit/slot/port convention, but system unit numbers are always 0, slot numbers are sequential, starting at 1, and the interface numbers (in the third position) are also sequential, starting at 1 per slot.



Note: Starting with SFTOS 2.5.1, LAGs (port channels) use the single integer ID that you assign when you create the LAG.

Other variations include:

- **Creating a static route:** The SFTOS command **ip route** supports only IP addresses for setting the next-hop router, while **ip route** in the FTOS also supports physical interfaces.
- **Setting the size of the logging buffer:** The FTOS command **logging buffered** has a parameter that enables you to set the size of the buffer, while SFTOS does not. Both FTOS and SFTOS invoke debug logging with the number 7 for the severity level parameter. The SFTOS command is **logging buffered 7**.
- **Displaying the MAC address table:** Both FTOS and SFTOS have the **show mac-address-table** command, but the SFTOS command **show mac-addr-table** provides more similar results to that FTOS command. The SFTOS syntax contains the *unit/slot/port* form cited above, for example, **show mac-addr-table interface 1/0/4**.
- **Displaying system information:** The FTOS command **show linecard** is similar to **show version** in SFTOS, which shows basic information, including the running software version and up time. Other similar commands in SFTOS are **show hardware** and **show sysinfo**, and **show tech-support** provides the results of a group of those similar commands.
- **service timestamps:** This FTOS command is not available in SFTOS. SFTOS sets timestamps automatically.
- **aaa authentication:** This FTOS command is available in SFTOS as **authentication**.

The iSupport Website

Access to some sections of the iSupport website do not require a password to access. However, if some section does require a password, you can request one at the iSupport website:

1. Click the **Support** link on the Force10 Networks home page: <http://www.force10networks.com>
2. Click the **Account Request** link.
3. Fill out the User Account Request form and click **Send**.
4. Click **Login**, and then enter the userid and password that you received by email.

The i-Support website (<http://www.force10networks.com/support/>) contains the following five tabs:

- **Home:** Summary of open cases, RMA management, and field notices (as shown below)
- **Service Request:** Case management
- **Software Center:** Software downloads, bug fixes, and bug tracking tool
- **Documents:** User documentation, FAQs, field notices, technical tips, and white papers
- **Support Programs:** Information on the suite of Force10 support and professional support services.

The screenshot shows the Force10 iSupport website interface. At the top, there is a navigation bar with links: PRODUCTS, APPLICATIONS, TECHNOLOGY, SUPPORT (highlighted), PARTNERS, NEWS/EVENTS, and COMPANY. Below this is a secondary bar with 'UPDATE MY PROFILE' and 'CUSTOMER SERVICE'. The main header features the 'FORCE10 iSUPPORT' logo and a set of tabs: HOME (selected), SERVICE REQUEST, SOFTWARE CENTER, DOCUMENTS, and SUPPORT PROGRAMS. On the left side, a user profile for 'Draviam Paramasivan' is shown with a 'LOGOUT' button. The main content area is titled 'Customer Support' and includes several sections: 'My Open Cases' with a table of open cases, 'My Open RMA' with a message about pending RMAs, 'Hot Topics' with a list of links, 'Field Alerts' with a list of security advisories, and 'Announcements' with links to bug track and FTOS version releases.

Case #	Title	Priority	Created On	Status
C-07026	test pl ignore	P4	05/28/2005	Close-Pending

Field Alerts

- [Force10 TCP Timestamp Security Advisory](#)
- [Force10 ICMP Attacks against TCP Advisory](#)
- [Mismatched Chassis Type on Redundant RPM](#)
- [Incorrect LC-EE3-RPM DIMM size](#)
- [Force10 TCP Security Advisory](#)

Hot Topics

- [FAQs](#)
- [Force10 Service and Support Guide](#)
- [Technical Tip: Restricting VTY Access](#)
- [Technical Tip: Adjusting MTU and Configuring Jumbo Frames Settings](#)

Announcements

- [Bug Track is Now Available](#)
- [FTOS Version 6.2.1.3 Release](#)

For more on using the iSupport website and accessing services, see the *Force10 Service and Support Guide*, available on the Home tab, as displayed above.

You can also contact the Force10 Technical Assistance Center (TAC) by email or phone. For details, click the **Contact Support** link on the Force10 Support page: <http://www.force10networks.com>

